PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-216830
(43)Date of publication of application : 04.08.2000

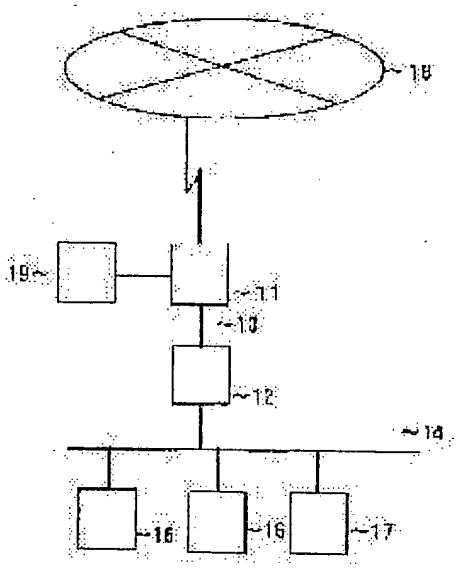
(51)Int.Cl. H04L 12/66
H04L 12/28
H04L 12/56

(21)Application number : 11-013977
(22)Date of filing : 22.01.1999

(71)Applicant : HITACHI LTD
(72)Inventor : NAMIKAWA TAKAKAZU

(54) MULTISTAGE FIRE WALL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To strengthen the security of an internal network against an intruder from outside in a computer system connected to a network.
SOLUTION: Plural fire walls 11, 12 are serially connected between an external network 18 and the internal network 14 and detect intrusion linking each other. In the case of judging abnormality at this time, the network of the respective fire walls 11, 12 is cut off to make it possible to protect the internal network 14 from access to the internal network 14 from outside.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－216830
(P2000－216830A)
(43)公開日　平成12年８月４日(2000.8.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｋ０３０
12/28		11/00	３１０Ｚ	５Ｋ０３３
12/56		11/20	１０２Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全５頁）

(21)出願番号　特願平11－13977

(22)出願日　平成11年１月22日(1999.1.22)

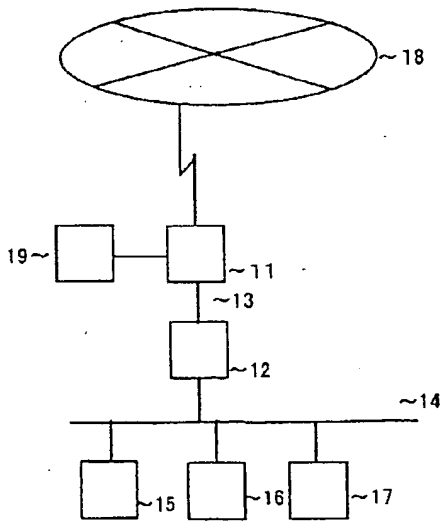
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　並河　孝和
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報システム事業部内
(74)代理人　100068504
弁理士　小川　勝男

Ｆターム(参考)　5K030 GA15 HC01 HC14 HD06
5K033 AA08 BA04 BA08 CB08 DA05

(54)【発明の名称】　多段ファイアウォールシステム

(57)【要約】
【課題】ネットワークに接続された計算機システムにおいて、外部からの侵入者に対して内部ネットワークのセキュリティを強化する。
【解決手段】外部ネットワークと内部ネットワークの間にファイアウォールを複数台直列に接続し、複数台のファイアウォールが連係して侵入の検知を行い、異常と判断した場合に各ファイアウォールのネットワークを切断することによって内部ネットワークへの外部からのアクセスに対して保護を行うことが可能になる。

図1



【特許請求の範囲】
【請求項１】外部ネットワークと内部ネットワークの間に、複数台の計算機を有する多段ファイアウォールシステムであって、前記計算機は内部状態を監視して異常を検知する監視手段と外部からのアクセスを検知する手段を備え、前記外部ネットワークに接続された計算機を経由して前記内部ネットワークに接続された前記計算機へのアクセスの検知をもって、前記外部ネットワークに接続された前記計算機の異常を把握することを特徴とした多段ファイアウォールシステム。
【請求項２】複数の前記計算機を直列に接続することで、外部ネットワークと内部ネットワークの経路を一つにすることを特徴とした請求項１記載の多段ファイアウォールシステム。
【請求項３】内部ネットワークに接続された前記計算機において、前記外部ネットワークに接続された計算機を経由したアクセスを検知した場合、あらかじめテーブルに登録しておいたアクセス以外のアクセスが検知された場合、外部ネットワークに接続された前記計算機のネットワーク接続および内部ネットワークに接続された前記計算機のネットワーク接続を切断することを特徴とした請求項１記載の多段ファイアウォールシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークに接続した計算機のセキュリティに関し、特に外部からファイアウォールへの侵入を検知し、さらに内部への侵入を防御するセキュリティシステムに関する。
【０００２】
【従来の技術】外部ネットワークからの侵入の防御策として、外部ネットワークと内部ネットワークの間にファイアウォールを設置し、（１）外部から使用できるサービスとユーザを限定するとともに、（２）アクセス記録を残しこれを監視することにより、内部ネットワークへの不正な侵入を防御する方法が主流である。インターネットとの接続において外部から使用できるサービスとユーザを限定する方法としては、インターネットとの通信のプロトコルであるTCP/IPのポート番号でサービスを限定し、ワンタイムパスワードや暗号化されたキー情報を使用したユーザ認証によって使用できるユーザを限定する方法がある。
【０００３】また、アクセス記録を残し監視する方法としては、オペレーティングシステムが記録するシステムログを定期的にチェックし異常を検知する方法や、ファイアウォールソフトがオペレーティングシステムのネットワークドライバを監視し許可されたＴＣＰ／ＩＰのポート番号以外のアクセス等の異常を検知するとともに記録に残す方法がある。
【０００４】従来の技術では、外部ネットワークと内部ネットワークの間にファイアウォールを設置し前述の方法で内部ネットワークへの不正な侵入を防御しているが、ファイアウォールに侵入が試みられた場合に、ファイアウォールで侵入を防御することに成功しているのか、ファイアウォールに侵入されて、侵入された記録も改竄されて異常が検知できていないのかの判断が出来ないという問題があった。
【０００５】この問題の解決策としては、特開平９－２１８３７号公報のようにネットワーク内の各々の計算機において侵入検知を行いセキュリティーの保護を実現する方法がある。しかし、この方法では各々の計算機に侵入検知の機能が必要となり、また侵入検知で異常が認められた場合の侵入の経路を特定することが難しく、また侵入された範囲を特定することが難しいといった問題があった。
【０００６】
【発明が解決しようとする課題】インターネットに接続することは、そのメリットを享受できるようになる反面、外部からの不正な侵入の脅威にさらされることになる。このような侵入に対する防御策として、外部ネットワークと内部ネットワークの間にファイアウォールを設置し、（１）外部から使用できるサービスとユーザを限定するとともに、（２）アクセス記録を残しこれを監視することにより、内部ネットワークへの不正な侵入を防御する方法が提案されている。
【０００７】しかし、このファイアウォールに万が一侵入されかつアクセス記録を何らかの方法で改竄された場合、外部からの侵入を検知できず、このファイアウォールから内部ネットワークに侵入することが可能になるという問題があった。
【０００８】そこで、本発明では、図１のようにファイアウォールを直列に複数個設置し、直前のファイアウォールへの侵入を監視することで、ファイアウォールに侵入されたことを検知することで、内部ネットワークの計算機に特別な機能を持たせることなく、内部ネットワークに対する侵入を未然に検知し、内部ネットワークのセキュリティを高めることを目的とする。
【０００９】
【課題を解決するための手段】上記課題を解決するために、本発明は、外部ネットワークと接続されているファイアウォール（外部ファイアウォール）と内部ネットワークに接続されているファイアウォール（内部ファイアウォール）およびその間の緩衝ネットワークにおいて、各ファイアウォールにて、外部からの侵入アクセスを検知する自己監視手段と、正常時のファイルシステムの状態と現在のファイルシステムの状態を相違を検出する整合性確認手段と、自己監視結果を内部ファイアウォールと管理者へ通知するメッセージの送受信手段を有し、外部ファイアウォールへの侵入を内部ファイアウォールで検知することを提供する。
【００１０】外部ファイアウォールに対し侵入が試みら

れた場合、外部ファイアウォールから内部ファイアウォールに対して、侵入が試みられたことを内部ファイアウォールへと通知し、その後、整合性確認を行いこの結果を内部ファイアウォールと管理者へ通知する。この時、外部ファイアウォールの整合性確認結果で侵入された形跡が認められた場合は、外部ファイアウォールと外部ネットワークを切断し、さらに内部ファイアウォールと緩衝ネットワークを切断するが、外部ファイアウォールの整合性確認結果で侵入された形跡が認められない場合でも、内部ファイアウォールに対して侵入が試みられた場合、外部ネットワークから内部ネットワークへの経路が一つしかないため、外部ファイアウォールは侵入されているため外部ファイアウォールと外部ネットワークを切断し、さらに内部ファイアウォールと緩衝ネットワークを切断する。

【００１１】

【発明の実施の形態】本発明の一実施の形態を図を用いて説明する。図１は本発明を適用した多段ファイアウォールの全体構成を示す図である。１８は外部ネットワーク（インターネット等）、１１は外部ネットワークに接続された外部ファイアウォールとしての計算機、１２は内部ネットワークに接続された内部ファイアウォールとしての計算機、１３は外部ファイアウォールと内部ファイアウォールを接続している緩衝ネットワーク、１４は内部ネットワーク、１５～１７は内部ネットワークに接続された計算機、１９は外部への情報発信のためのサーバ（WWWサーバ、FTPサーバ等）としての計算機である。ただし、１９は外部ネットワークに対して情報発信を行う場合のみ設置する計算機である。外部ネットワーク１８から内部ネットワーク１４に侵入するためには、必ず計算機１１および１２を通過する必要がある。

【００１２】本発明においては、これまでファイアウォールを設置していた箇所に２台以上のファイアウォールとしての計算機を設置し、この計算機が連係して動作することで、外部からの不正侵入の検知を実現する。計算機の連係については、後述する。また、計算機１１と計算機１２は、それぞれの計算機のネットワークドライバを含むオペレーティングシステムとハードディスクが独立して機能すれば、一つの筐体に納めることも可能である。

【００１３】図２は図１の多段ファイアウォールシステムで使用する計算機１１および計算機１２の概要を示す図である。２１は図１の計算機１１または計算機１２である。２２はアクセス監視部、２３はアクセス管理テーブル、２４は整合性確認部、２５は整合性データベース、２６はオペレーティングシステム、２７はシステムロギング部、２８はプロセス管理部、２９及び２１０はネットワークドライバ、２１１はファイルシステム制御ドライバ、２１２は情報伝達部、２１３は計算機１１の場合は図１における外部ネットワーク１８、計算機１２の場合は図１における緩衝ネットワーク１３、２１４は計算機１１の場合は図１の緩衝ネットワーク１３、計算機１２の場合は図１における内部ネットワーク１４である。

【００１４】アクセス監視部は、オペレーティングシステムを監視し、アクセス管理テーブルに基づいてアクセスを制御するとともに、アクセス記録を残す。またアクセス監視部は、オペレーティングシステムが持つシステムロギングの記録を監視しており、アクセス管理テーブルの内容と比較して侵入の試みを検知する。整合性確認部は、正常時のシステムの情報を整合性データベースとして持ち、正常時の整合性データベースと現在のシステムの情報を比較して侵入者によるシステムの改竄を検知する。

【００１５】情報伝達部は、メッセージの着信監視を常に行っている。情報伝達部は、侵入の試みやシステムの改竄が検知された場合に、あらかじめ登録してある計算機と管理者へメッセージを送信する。また情報伝達部は、オペレーティングシステムの任意のネットワークドライバを停止する機能を持ち、ネットワークを切断することを可能にする。外部ネットワークへの情報発信を行う場合には、情報発信を行う計算機を接続するネットワークドライバは、２９及び２１０以外に必要となる。

【００１６】図３は図１に示した計算機１１で実行される不正アクセス発生時の状態監視の処理のフローチャートである。計算機１１ではアクセス監視部がアクセス監視を行っており（ステップ３１）、アクセス監視部より不正アクセスが検知された場合（ステップ３２）、情報伝達部が内部ファイアウォール及び管理者にアクセスメッセージ通知を行う（ステップ３３）。これは、UNIXの場合、sendmailを使用してアクセス通知を行うことが可能である。

【００１７】アクセス通知を行った後、計算機１１で整合性確認部が、あらかじめ内部に持っている正常時の整合性データベースと現在の情報を比較する整合性確認を行う（ステップ３４）。整合性確認の結果を判断し（ステップ３５）、正常時の整合性データベースと現在の情報に相違が有った場合、侵入によって異常が発生したとして、計算機１２と管理者に侵入メッセージを通知する（ステップ３６）。この通知もアクセスメッセージ通知の場合と同様にUNIXの場合は、sendmailを使用して侵入メッセージ通知を行うことが可能である。

【００１８】侵入メッセージの通知を行った後、計算機１１は外部ネットワークと接続しているネットワークドライバを停止することで、ネットワークを切断する（ステップ３７）。ステップ３５の判断で相違がない場合は、ステップ３１に戻り、アクセス監視状態になる。

【００１９】図４は、計算機１２において、計算機１１からアクセスメッセージ通知を受けた場合に実行される計算機１２での状態監視の処理のフローチャートであ

る。計算機１２の情報伝達部にて計算機１１からのアクセスメッセージ通知を受け取った（ステップ４１）場合、計算機１２において整合性確認部が、あらかじめ内部に持っている正常時の整合性データベースと現在の情報を比較する整合性確認を行う（ステップ４２）。

【００２０】整合性確認の結果を判断し（ステップ４３）、正常時の整合性データベースと現在の情報に相違が有った場合、侵入によって異常が発生したとして、計算機１１と管理者に侵入メッセージを通知する（ステップ４４）。この通知はUNIXの場合は、sendmailを使用して侵入メッセージ通知を行うことが可能である。

【００２１】侵入メッセージの通知を行った後、計算機１２は計算機１１と接続しているネットワークドライバを停止することで、ネットワークを切断する（ステップ４５）。ステップ４３の判断で相違がない場合は、処理を終了する。

【００２２】図５は、計算機１２において、不正なアクセスが発生した場合に実行される計算機１２でのアクセス制御の処理のフローチャートである。計算機１２においても、計算機１１と同様にアクセス監視を実施しており、計算機１２に対する不正アクセスが発生した場合（ステップ５１）、計算機１２に対して侵入者がアクセスを試みるには、計算機１２と計算機１１の経路が一つしかないため計算機１１からアクセスする必要があるため、すでに計算機１１は外部から侵入されていると判断し、計算機１２の情報伝達部が計算機１１及び管理者に対し侵入メッセージを通知し（ステップ５２）、計算機１２は計算機１１と接続しているネットワークドライバを停止することで、ネットワークを切断する（ステップ５３）。

【００２３】図６は、計算機１１又は計算機１２において、情報伝達部が侵入メッセージを受け取った場合に計算機１１または計算機１２で実行されるアクセス制御の処理のフローチャートである。情報伝達部で侵入メッセージを受け取った場合（ステップ６１）、計算機は外部ネットワーク又は、計算機１１と接続しているネットワークドライバを停止することで、ネットワークを切断する（ステップ６２）。

【００２４】

【発明の効果】以上のように、本発明においては、これまでファイアウォールを設置していた箇所に２台以上のファイアウォールとしての計算機を設置し、この計算機が連係して動作することで、外部からの不正侵入の検知を実現する。

【図面の簡単な説明】

【図１】本発明が適用されるネットワークシステムの全体構成を示すブロック図。

【図２】図１の計算機１１および計算機１２の構成例を示すブロック図。

【図３】図１の計算機１１における不正アクセス発生時の状態監視処理のフローチャート。

【図４】図１の計算機１２においてアクセスメッセージ通知を受けた場合の状態監視処理のフローチャート。

【図５】図１の計算機１２において不正アクセス発生時のアクセス制御処理のフローチャート。

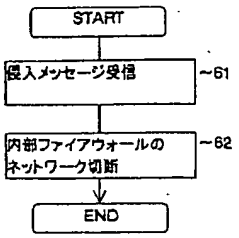
【図６】図２の計算機において侵入メッセージを受け取った場合のアクセス制御処理のフローチャート。

【符号の説明】

１１…外部ファイアウォール、１２…内部ファイアウォール、１３…緩衝ネットワーク、１４…内部ネットワーク、１５～１７…計算機、１８…外部ネットワーク、１９…外部情報発信のための計算機、２１…ファイアウォール、２２…アクセス監視部、２３…アクセス管理テーブル、２４…整合性確認部、２５…整合性データベース、２６…オペレーティングシステム、２７…システムロギング部、２８…プロセス管理部、２９～２１０…ネットワークドライバ、２１１…ファイルシステム制御ドライバ、２１２…情報伝達部、２１３～２１４…ネットワーク、３１…アクセス監視処理、３２…不正アクセス検知処理、３３…アクセスメッセージ通知処理、３４…整合性確認処理、３５…整合性確認結果判断処理、３６…侵入メッセージ通知処理、３７…ネットワーク切断処理、４１…メッセージ受信処理、４２…整合性確認処理、４３…整合性結果確認処理、４４…侵入メッセージ通知処理、４５…ネットワーク切断処理、５１…不正アクセス検知処理、５２…侵入メッセージ通知処理、５３…ネットワーク切断処理、６１…メッセージ受信処理、６２…ネットワーク切断処理。

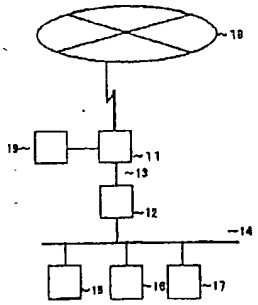
【図６】

図６



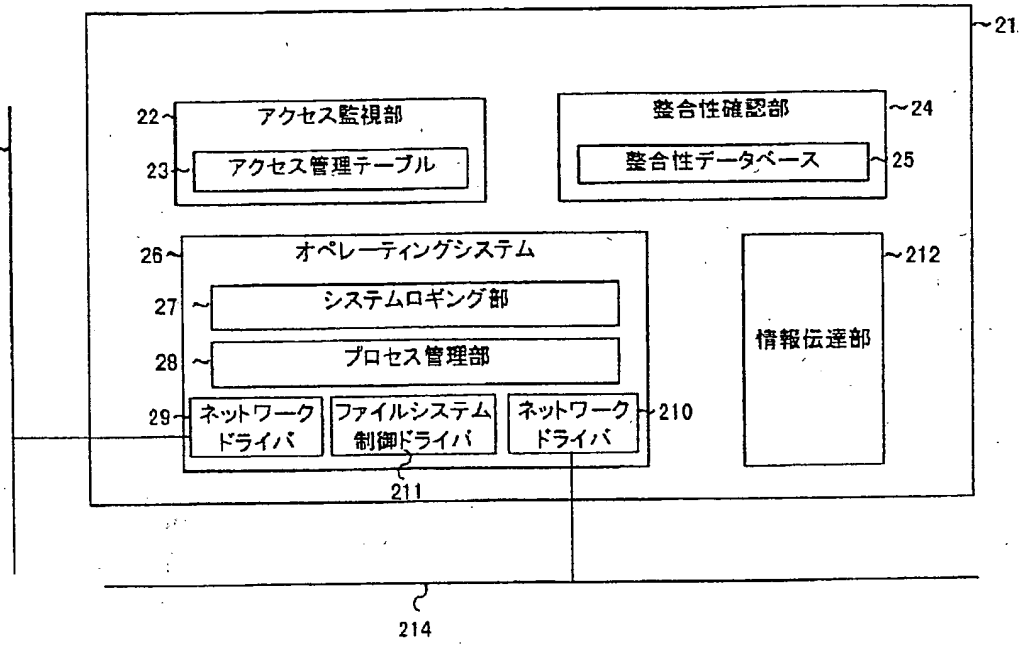
【図１】

図1



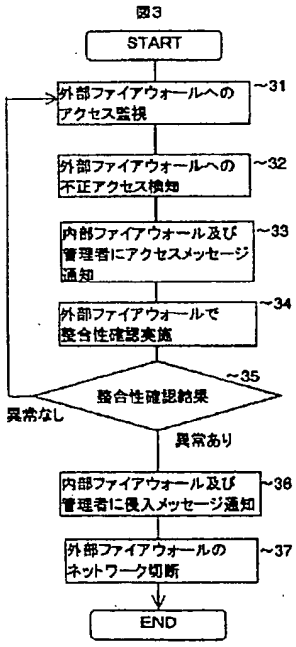
【図２】

図2



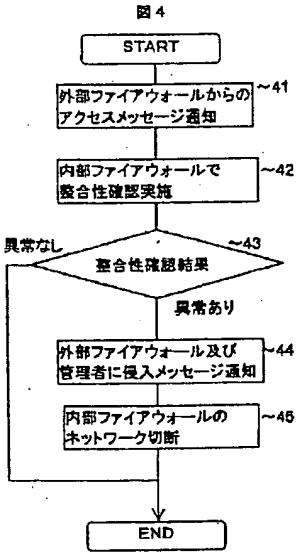
【図３】

図3



【図４】

図4



【図５】

図5